



PATENT ABSTRACTS OF JAPAN

(11) Publication number: **11154184 A**(43) Date of publication of application: **08.06.99**

(51) Int. Cl. **G06F 17/60**
G06F 15/00
// G09C 1/00

(21) Application number: **09322833**(22) Date of filing: **25.11.97**

(71) Applicant: **NIPPON TELEGR & TELEPH**
CORP <NTT> NTT
ELECTRONICS CORP

(72) Inventor: **TAKADA SHUNSUKE**
KAWAKUBO HIDEJI
YAMANAKA KIYOSHI
MATSUMOTO HIROYUKI

(54) **METHOD AND SYSTEM FOR MANAGING**
SAFETY OF INFORMATION DISTRIBUTION

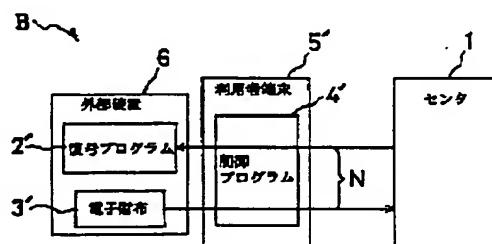
various kinds of information is separately connected to the user terminal 5'.

(57) Abstract:

COPYRIGHT: (C)1999,JPO

PROBLEM TO BE SOLVED: To provide a method and a system for managing safety of information distribution with which contents can be safely delivered and utilized in the information distribution in electronic commercial transaction.

SOLUTION: A center 1 having an enciphered distribution sales function, advertisement and propaganda function and payment collection settlement function and a user terminal 5' having a control program 4' for controlling an enciphered distribution purchase function, transfer function and drawing-out/ payment enciphering function are mutually connected by an information communication network N, and an external device 6 having a deciphering program 2' for deciphering enciphered sales contents Ke [M], which is transferred from the user terminal 5', with a previously or simultaneously transferred content cryptographic key Kup [Ke] enciphered in advance by operating while being interlocked with the control program 4', electronic wallet 3' for updating, enciphering and storing the payment subtracted remainder, and function for enciphering and storing



(51)Int.Cl.⁵

識別記号

F I

G 0 6 F 17/60

G 0 6 F 15/21

3 3 0

15/00

3 3 0

15/00

3 3 0 Z

// G 0 9 C 1/00

6 6 0

G 0 9 C 1/00

6 6 0 F

6 6 0 B

審査請求 未請求 請求項の数24 O L (全 10 頁)

(21)出願番号

特願平9-322833

(22)出願日

平成9年(1997)11月25日

(71)出願人 000004226

日本電信電話株式会社

東京都新宿区西新宿三丁目19番2号

(71)出願人 591230295

エヌティティエレクトロニクス株式会社

東京都渋谷区桜丘町20番1号

(72)発明者 高田 俊介

東京都新宿区西新宿三丁目19番2号 日本

電信電話株式会社内

(72)発明者 河久保 秀二

東京都新宿区西新宿三丁目19番2号 日本

電信電話株式会社内

(74)代理人 弁理士 菅 隆彦

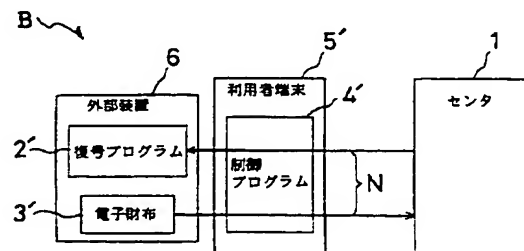
最終頁に続く

(54)【発明の名称】 情報流通安全管理方法及びシステム

(57)【要約】

【課題】電子商取引の情報流通において、コンテンツを安全に配送し利用し得る情報流通安全管理方法及びシステムの提供。

【解決手段】暗号化流通販売機能と広告宣伝機能と代金回収決算機能を有するセンタ1と、暗号化流通購入機能と転送機能と代金引出し支払い暗号化機能を制御する制御プログラム4'を有する利用者端末5'と間を情報通信網Nで相互接続し、制御プログラム4'に連携作動して利用者端末5'から転送された暗号化販売コンテンツKe[M]を先又は同時に転送され事前に復号化されたコンテンツ暗号鍵Kup[Ke]で復号化処理する復号プログラム2'と、代金差引残高を更新暗号化記憶する電子財布3'と、各種情報の暗号化記憶機能と、を有する外部装置6を利用者端末5'に分離接続するシステム構成の特徴。



【特許請求の範囲】

【請求項1】販売コンテンツを有するセンタから情報通信網を介して店頭公開流通された広告宣伝用コンテンツ情報を利用者端末手段でアクセス閲覧して前記センタに購入要求し、当該利用者端末手段に配送された暗号化販売コンテンツの復号化処理及び電子決済処理の一連の電子商取引を行うに当り、

当該復号化処理及び当該電子決済処理の内の電子財布保管処理は、前記利用者端末と切離し、相互にプログラム連携して安全確保された外部処理に委ねられる、ことを特徴とする情報流通安全管理方法。

【請求項2】店頭公開された広告宣伝用コンテンツ情報は、情報購買意欲を湧かせるために、販売コンテンツが容易に推測出来、かつネットワーク負荷が小さい再編情報である、ことを特徴とする請求項1に記載の情報流通安全管理方法。

【請求項3】センタ及び利用者端末は、一連の電子商取引に公開鍵暗号方式を利用する、ことを特徴とする請求項1又は2に記載の情報流通安全管理方法。

【請求項4】センタ及び利用者端末は、それぞれ自己の秘密鍵を自己保持し、自己の公開鍵を相手に公開する、ことを特徴とする請求項3に記載の情報流通安全管理方法。

【請求項5】配送された暗号化販売コンテンツは、配送時に配送毎にランダムに生成されたコンテンツ暗号鍵で暗号化する、ことを特徴とする請求項1、2、3又は4に記載の情報流通安全管理方法。

【請求項6】相互のプログラム連携は、利用者端末の制御プログラムと外部処理の復号プログラム及び電子財布間で行われる、ことを特徴とする請求項1、2、3、4又は5に記載の情報流通安全管理方法。

【請求項7】電子財布は、電子クーポンや電子チケットや電子小切手やビットキャッシュやクレジットカードやサイバーコイン等の暗号化残高情報を記憶保管する、ことを特徴とする請求項6に記載の情報流通安全管理方法。

【請求項8】販売コンテンツは、文書情報、画像情報、音声情報、これらの組合せ情報である、ことを特徴とする請求項1、2、3、4、5、6又は7に記載の情報流通安全管理方法。

【請求項9】復号化処理は、復号鍵及び秘密鍵を漏洩させない機密保護領域内で実行

される、

ことを特徴とする請求項1、2、3、4、5、6、7又は8に記載の情報流通安全管理方法。

【請求項10】外部処理は、マネー、コンテンツ、コンテンツ暗号鍵及び秘密鍵の全情報をマスター鍵にて機密保護領域内で暗号化されて記憶する、

ことを特徴とする請求項1、2、3、4、5、6、7、8又は9に記載の情報流通安全管理方法。

10 【請求項11】マスター鍵は、機密保護領域内に記憶保持される、ことを特徴とする請求項10に記載の情報流通安全管理方法。

【請求項12】マネー、コンテンツ、暗号鍵及び秘密鍵の全情報は、機密保護領域外に記憶保持される、ことを特徴とする請求項10又は11に記載の情報流通安全管理方法。

20 【請求項13】センタは、ストアやショップ、ショッピングセンタ、コミュニケーションセンタ、ショッピングモール、図書館、資料館、雑誌社、出版社、放送局、レコード会社、ゲームソフト会社、映画会社、新聞社等のヴァーチャル及びリアルを含む、ことを特徴とする請求項1、2、3、4、5、6、7、8、9、10、11又は12に記載の情報流通安全管理方法。

30 【請求項14】情報通信網は、インターネット、イントラネット（販売部を有する）、LAN、VAN、ISDN、VPN等を含む、ことを特徴とする請求項1、2、3、4、5、6、7、8、9、10、11、12又は13に記載の情報流通安全管理方法。

40 【請求項15】センタ側では予め販売コンテンツを登録して置くステップ1（ST1）と、当該販売コンテンツに基づき広告宣伝用コンテンツ情報を再編生成するステップ2（ST2）と、当該広告宣伝用コンテンツ情報を利用者端末向に店頭公開するステップ3（ST3）と、利用者端末でアクセス操作して当該広告宣伝用コンテンツ情報を閲覧するステップ4（ST4）と、検討の上前記センタに購入要求するステップ5（ST5）と、購入要求を受けた当該センタは乱数表等にて暗号鍵を生成するステップ6（ST6）と、当該暗号鍵で前記販売コンテンツを暗号化処理するステップ7（ST7）と、当該暗号化販売コンテンツと公開鍵で暗号化した当該暗号鍵を利用者端末に送信するステップ8（ST8）と、当該暗号化販売コンテンツと当該暗号化暗号鍵とを受け

た利用者端末は外部処理に回すステップ9 (ST9) と、
 当該外部処理において、自己保持秘密鍵で復号化した前記暗号鍵で暗号化販売コンテンツを復号化処理してコンテンツを取得するステップ10 (ST10) と、
 前記外部処理で保管された電子財布から代金を利用者端末で引出して、前記センタに暗号化送信するステップ11 (ST11) と、
 代金を受信した前記センタは復号化決算処理するステップ12 (ST12) と、
 を順次踏んで実行処理する、
 ことを特徴とする情報流通安全管理方法。
 【請求項16】販売コンテンツを登録し、広告宣伝用コンテンツを店頭公開流通するとともに購入要求に対し、公開鍵で暗号化したコンテンツ暗号鍵と当該コンテンツ暗号鍵で暗号化した販売コンテンツを送信して見返りに受信した代金を復号化決算処理するセンタと、
 前記広告宣伝用コンテンツをアクセス閲覧して当該センタへ購入要求を応信し、返信してきた前記暗号化販売コンテンツと前記暗号化暗号鍵とを転信し、対価を引出して暗号化支払いを行う制御プログラムを有する利用者端末と、
 前記センタと当該利用者端末とを結ぶ情報通信網と、
 前記制御プログラムに連動作動する復号プログラムと電子財布とを有し、前記利用者端末から転送されてきた前記暗号化コンテンツを、自己保持秘密鍵で復号化した前記暗号鍵で復号化し、再度暗号化記憶するとともに前記電子財布に記憶保持される電子マネーの代金差引残高を更新暗号化記憶する外部装置と、を備える、
 ことを特徴とする情報流通安全管理システム。
 【請求項17】外部装置は、
 暗号化コンテンツと暗号化コンテンツ暗号鍵を受信する端末入出力制御部と、
 一連の復号、暗号及び記憶機能を統御する制御部と、
 前記暗号化コンテンツ暗号鍵を自己保持秘密鍵で復号する暗号鍵復号部と、
 前記暗号化販売コンテンツを当該コンテンツ暗号鍵でコンテンツに復号するコンテンツ復号部と、
 マスター鍵を記憶保持するマスター記憶部と、
 マネー、前記コンテンツ、前記コンテンツ暗号鍵及び前記秘密鍵の全情報を前記マスター鍵で暗号化又は復号化する暗号／復号部と、
 暗号化された前記マネー情報を記憶するマネー情報記憶部と、
 暗号化された前記コンテンツ情報を記憶するコンテンツ情報記憶部と、
 暗号化された前記コンテンツ暗号鍵を記憶する暗号鍵記憶部と、
 暗号化された前記秘密鍵を記憶する秘密鍵記憶部と、から構成される、

ことを特徴とする請求項16に記載の情報流通安全管理システム。

【請求項18】制御部とコンテンツ復号部とマスター鍵記憶部と暗号／復号部と暗号鍵復号部は、
 外部装置に内蔵された機密保護装置内に収められている、

ことを特徴とする請求項17に記載の情報流通安全管理システム。

【請求項19】マネー情報記憶部は、

10 電子クーポンや電子チケットや電子小切手やビットキャッシュやクレジットカードやサイバーコイン等の暗号化残高情報を記憶保持する機能を備える、

ことを特徴とする請求項17又は18に記載の情報流通安全管理システム。

【請求項20】秘密鍵記憶部は、

公開鍵暗号方式の暗号化秘密鍵を記憶する機能を備える、

ことを特徴とする請求項17、18又は19に記載の情報流通安全管理システム。

20 【請求項21】コンテンツ情報記憶部は、

それぞれ暗号化文書情報、暗号化画像情報、暗号化音声情報、これ等の組合せ暗号化情報を記憶する機能を備える、

ことを特徴とする請求項17、18、19又は20に記載の情報流通安全管理システム。

【請求項22】暗号鍵記憶部は、

暗号化コンテンツ暗号鍵を記憶する機能を備える、

ことを特徴とする請求項17、18、19、20又は21に記載の情報流通安全管理システム。

30 【請求項23】情報通信網は、

インターネット、イントラネット（販売部を有する）、LAN、VAN、ISDN、VPN等を含む、

ことを特徴とする請求項16、17、18、19、20、21又は22に記載の情報流通安全管理システム。

【請求項24】センタは、

ストアやショップ、ショッピングセンタ、コミュニケーションセンタ、ショッピングモール、図書館、資料館、雑誌社、出版社、放送局、レコード会社、ゲームソフト会社、映画会社、新聞社等のヴァーチャル及びリアルを含む、

40 ことを特徴とする請求項16、17、18、19、20、21、22又は23に記載の情報流通安全管理システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、インターネット等の情報通信網を利用した情報流通安全管理方法及びその実施に直接使用するシステムに関する。

【0002】

50 【従来の技術】従来の情報流通システムAは図4に示す

よう、暗号化販売コンテンツ情報を店頭公開するセンタ 1 と、当該暗号化販売コンテンツ情報をアクセス閲覧し復号する復号プログラム 2 と、センタ 1 への送金用の電子財布 3 とを収めた制御プログラム 4 を保有する利用者端末 5 で構成される。

【0003】当該情報流通システム A の処理手順方法は、図 5 に示すようセンタ 1 側では、予め販売情報としてのコンテンツ M 情報を登録して置き (STA)、その都度暗号鍵 Ke を生成して (STB)、コンテンツ M を暗号鍵 Ke で暗号化し (STC)、暗号化販売コンテンツ Ke [M] を利用者端末 5 側に対し直接店頭公開する (STD)。

【0004】次いで、利用者端末 5 側では、アクセス操作して暗号化販売コンテンツ Ke [M] を閲覧し (STE)、制御プログラム 4 を駆動して、検討の上、購入要求をセンタ 1 に送信すれば (STF)、センタ 1 は受注を確認して暗号鍵 Ke を送信する (STG)。引続き、利用者端末 5 で暗号鍵 Ke を受けると復号プログラム 2 を駆動して保持していた暗号化販売コンテンツ Ke [M] を暗号鍵 Ke で復号処理し、コンテンツ M を得る (STH)。

【0005】その上で、その対価支払いとして制御プログラム 4 により電子財布 3 からセンタ 1 向けに代金送信し (STI)、センタ 1 では、送金を受けて決算処理し (STJ)、センタ 1 と利用者端末 5 間の電子商取引を終了する。

【0006】

【発明が解決しようとする課題】以上の通り、従来の情報流通システム A では、予め原サイズコンテンツ M 情報の情報全部に特定の暗号鍵 Ke でモザイクや暗号化したコンテンツ M 情報を利用者に店頭公開し、利用者からの購入要求後に復号鍵 Ke を送信するため、容易に原サイズコンテンツ M 情報を推測出来ず、購買意欲が湧かないとともに、情報転送量が多く、最終的に利用者が購入しなかった場合の転送処理が無駄になり、しかも暗号鍵 Ke が盗まれると他の利用者が購入した該コンテンツ M 情報も不正利用される。

【0007】又、利用者端末 5 内でコンテンツ M 情報を復号するため、利用者端末 5 や復号プログラム 2 に不正を行われると復号鍵 Ke が盗まれるとともに、利用者端末 5 内の購入コンテンツ M 情報を消去され、さらには電子クーポンやチケットなどの電子財布 3 情報を消去される危険を有する。

【0008】ここにおいて、本発明の解決すべき主要な目的は次の通りである。即ち、本発明の第 1 の目的は、電子商取引の情報流通において、コンテンツを安全に配送し利用し得る情報流通安全管理方法及びシステムを提供せんとするものである。

【0009】本発明の第 2 の目的は、電子商取引に先立って、電子広告宣伝し、購買意欲をそそって商売繁盛を

もたらす情報流通安全管理方法及びシステムを提供せんとするものである。

【0010】本発明の第 3 の目的は、販売コンテンツ情報に関する広告宣伝用コンテンツ情報に誇張化、書き換え等再編して店頭公開情報の転送量を少なくし合理化、効率化、経済化を計った情報流通安全管理方法及びシステムを提供せんとするものである。

【0011】本発明の第 4 の目的は、利用者側の安全を要する復号処理及び電子マネー保管処理を利用者端末とは切離し連携した外部処理で行う情報流通安全管理方法及びシステムを提供せんとするものである。

【0012】本発明のその他の目的は、明細書、図面、特に、特許請求の範囲の各請求項の記載から自ずと明かとなろう。

【0013】

【課題を解決するための手段】本発明は、前記課題を解決するに当り、暗号化流通販売機能、広告宣伝機能及び代金回収復号化決算機能を有するセンタと、暗号化流通購入機能と転送機能と代金引出し暗号化支払い機能を制御する制御プログラムを有する利用者端末と間を情報通信網で接続し、前記制御プログラムに連携動作して前記利用者端末から転送された暗号化コンテンツを、先又は同時に転送され事前に復号化されたコンテンツ暗号鍵で復号化処理する復号プログラミングと代金差し引き残高を更新暗号化記憶する電子財布と、各種情報の暗号化記憶機能と、を有する外部装置を前記利用者端末に分離接続するシステム構成を採用する。

【0014】そして、利用者に情報を店頭公開する際、情報購買意欲を湧かせるために原情報が容易に推測でき、かつサイズの小さい情報を公開するとともに、情報配送時に乱数表等にて生成したセッション鍵を暗号化する一方、情報復号を外部装置の機密保護装置で行い、復号鍵を漏洩させない。しかも、購入情報を外部装置に保持させ、電子マネーとして電子クーポンや電子チケット等の残高情報を外部装置内の電子財布に安全に保持する。

【0015】さらに、具体的詳細に述べれば、本発明が、当該課題解決のため、次に列挙する上位概念から下位概念に互る新規な特徴的構成手法又は手段を採用することにより、前記目的を達成する。

【0016】即ち、本発明方法の第 1 の特徴は、販売コンテンツを有するセンタから情報通信網を介して店頭公開流通された広告宣伝用コンテンツ情報を利用者端末手段でアクセス閲覧して前記センタに購入要求し、当該利用者端末手段に配送された暗号化販売コンテンツの復号化処理及び電子決算処理の一連の電子商取引を行うに当り、当該復号化処理及び当該電子決算処理の内の電子財布保管処理は、前記利用者端末と切離し、相互にプログラム連携して安全確保された外部処理に委ねられてなる情報流通安全管理方法の構成採用にある。

【0017】本発明方法の第2の特徴は、前記本発明方法の第1の特徴における店頭公開された広告宣伝用コンテンツ情報が、情報購買意欲を湧かせるために、販売コンテンツが容易に推測出来、かつネットワーク負荷が小さい再編情報である情報流通安全管理方法の構成採用にある。

【0018】本発明方法の第3の特徴は、前記本発明方法の第1又は第2の特徴におけるセンタ及び利用者端末が、一連の電子商取引に公開鍵暗号方式を利用してなる情報流通安全管理方法の構成採用にある。

【0019】本発明方法の第4の特徴は、前記本発明方法の第3の特徴におけるセンタ及び利用者端末が、それぞれ自己の秘密鍵を自己保持し、自己の公開鍵を相手に公開してなる情報流通安全管理方法の構成採用にある。

【0020】本発明方法の第5の特徴は、前記本発明方法の第1、第2、第3又は第4の特徴における配送された暗号化販売コンテンツが、配送時に配送毎にランダムに生成されたコンテンツ暗号鍵で暗号化してなる情報流通安全管理方法の構成採用にある。

【0021】本発明方法の第6の特徴は、前記本発明方法の第1、第2、第3、第4又は第5の特徴における相互のプログラム連携が、利用者端末の制御プログラムと外部処理の復号プログラム及び電子財布間で行われてなる情報流通安全管理方法の構成採用にある。

【0022】本発明方法の第7の特徴は、前記本発明方法の第6の特徴における電子財布が、電子クーポンや電子チケットや電子小切手やビットキャッシュやクレジットカードやサイバーコイン等の暗号化残高情報を記憶保持してなる情報流通安全管理方法の構成採用にある。

【0023】本発明方法の第8の特徴は、前記本発明方法の第1、第2、第3、第4、第5、第6又は第7の特徴における販売コンテンツが、文書情報、画像情報、音声情報、これらの組合せ情報である情報流通安全管理方法の構成採用にある。

【0024】本発明方法の第9の特徴は、前記本発明方法の第1、第2、第3、第4、第5、第6、第7又は第8の特徴における復号化処理が、復号鍵及び秘密鍵を漏洩させない機密保護領域内で実行されてなる情報流通安全管理方法の構成採用にある。

【0025】本発明方法の第10の特徴は、前記本発明方法の第1、第2、第3、第4、第5、第6、第7、第8又は第9の特徴における外部処理が、マネー、コンテンツ、コンテンツ暗号鍵及び秘密鍵の全情報をマスター鍵にて機密保護領域内で暗号化されて記憶してなる情報流通安全管理方法の構成採用にある。

【0026】本発明方法の第11の特徴は、前記本発明方法の第10の特徴におけるマスター鍵が、機密保護領域内に記憶保持されてなる情報流通安全管理方法の構成採用にある。

【0027】本発明方法の第12の特徴は、前記本発明

方法の第10又は第11の特徴におけるマネー、コンテンツ、暗号鍵及び秘密鍵の全情報が、機密保護領域外に記憶保持されてなる情報流通安全管理方法の構成採用にある。

【0028】本発明方法の第13の特徴は、前記本発明方法の第1、第2、第3、第4、第5、第6、第7、第8、第9、第10、第11又は第12の特徴におけるセンタが、ストアやショップ、ショッピングセンタ、コミュニケーションセンタ、ショッピングモール、図書館、資料館、雑誌社、出版社、放送局、レコード会社、ゲームソフト会社、映画会社、新聞社等のヴァーチャル及びリアルを含んでなる情報流通安全管理方法の構成採用にある。

【0029】本発明方法の第14の特徴は、前記本発明方法の第1、第2、第3、第4、第5、第6、第7、第8、第9、第10、第11、第12又は第13の特徴における情報通信網が、インターネット、イントラネット（販売部を有する）、LAN、VAN、ISDN、VPN等を含んでなる情報流通安全管理方法の構成採用にある。

【0030】本発明方法の第15の特徴は、センタ側では予め販売コンテンツを登録して置くステップ1（ST1）と、当該販売コンテンツに基づき広告宣伝用コンテンツ情報を再編生成するステップ2（ST2）と、当該広告宣伝用コンテンツ情報を利用者端末向に店頭公開するステップ3（ST3）と、利用者端末でアクセス操作して当該広告宣伝用コンテンツ情報を閲覧するステップ4（ST4）と、検討の上前記センタに購入要求するステップ5（ST5）と、購入要求を受けた当該センタは乱数表等にて暗号鍵を生成するステップ6（ST6）と、当該暗号鍵で前記販売コンテンツを暗号化処理するステップ7（ST7）と、当該暗号化販売コンテンツと公開鍵で暗号化した当該暗号鍵を利用者端末に送信するステップ8（ST8）と、当該暗号化販売コンテンツと当該暗号化暗号鍵とを受けた利用者端末は外部処理に回すステップ9（ST9）と、当該外部処理において、自己保持秘密鍵で復号化した前記暗号鍵で暗号化販売コンテンツを復号化処理してコンテンツを取得するステップ10（ST10）と、前記外部処理で保管された電子財布から代金を利用者端末で引出して、前記センタに暗号化送信するステップ11（ST11）と、代金を受信した前記センタは復号化決算処理するステップ12（ST12）と、を順次踏んで実行処理してなる情報流通安全管理方法の構成採用にある。

【0031】本発明システムの第1の特徴は、販売コンテンツを登録し、広告宣伝用コンテンツを店頭公開流通するとともに購入要求に対し、公開鍵で暗号化したコンテンツ暗号鍵と当該コンテンツ暗号鍵で暗号化した販売コンテンツを送信して見返りに受信した代金を復号化決算処理するセンタと、前記広告宣伝用コンテンツをアク

セス閲覧して当該センタへ購入要求を応信し、返信してきた前記暗号化販売コンテンツと前記暗号化暗号鍵とを転信し、対価を引出して暗号化支払いを行う制御プログラムを有する利用者端末と、前記センタと当該利用者端末とを結ぶ情報通信網と、前記制御プログラムに連携動作する復号プログラムと電子財布とを有し、前記利用者端末から転送されてきた前記暗号化コンテンツを、自己保持秘密鍵で復号化した前記暗号鍵で復号化し、再度暗号化記憶するとともに前記電子財布に記憶保持される電子マネーの代金差引残高を更新暗号化記憶する外部装置と、を備えてなる情報流通安全管理システムの構成採用にある。

【0032】本発明システムの第2の特徴は、前記本発明システムの第1の特徴における外部装置が、暗号化コンテンツと暗号化コンテンツ暗号鍵を受信する端末入出力制御部と、一連の復号、暗号及び記憶機能を統御する制御部と、前記暗号化コンテンツ暗号鍵を自己保持秘密鍵で復号する暗号鍵復号部と、前記暗号化販売コンテンツを当該コンテンツ暗号鍵でコンテンツに復号するコンテンツ復号部と、マスター鍵を記憶保持するマスター記憶部と、マネー、前記コンテンツ、前記コンテンツ暗号鍵及び前記秘密鍵の全情報を前記マスター鍵で暗号化又は復号化する暗号／復号部と、暗号化された前記マネー情報を記憶するマネー情報記憶部と、暗号化された前記コンテンツ情報を記憶するコンテンツ情報記憶部と、暗号化された前記コンテンツ暗号鍵を記憶する暗号鍵記憶部と、暗号化された前記秘密鍵を記憶する秘密鍵記憶部と、から構成されてなる情報流通安全管理システムの構成採用にある。

【0033】本発明システムの第3の特徴は、前記本発明システムの第2の特徴における制御部とコンテンツ復号部とマスター鍵記憶部と暗号／復号部と暗号鍵復号部とが、外部装置に内蔵された機密保護装置内に収められてなる情報流通安全管理システムの構成採用にある。

【0034】本発明システムの第4の特徴は、前記本発明システムの第2又は第3の特徴におけるマネー情報記憶部が、電子クーポンや電子チケットや電子小切手やビットキャッシュやクレジットカードやサイバーコイン等の暗号化残高情報を記憶保持する機能を備えてなる情報流通安全管理システムの構成採用にある。

【0035】本発明システムの第5の特徴は、前記本発明システムの第2、第3又は第4の特徴における秘密鍵記憶部が、公開鍵暗号方式の暗号化秘密鍵を記憶する機能を備えてなる情報流通安全管理システムの構成採用にある。

【0036】本発明システムの第6の特徴は、前記本発明システムの第2、第3、第4又は第5の特徴におけるコンテンツ情報記憶部が、それぞれ暗号化文書情報、暗号化画像情報、暗号化音声情報、これ等の組合せ暗号化情報を記憶する機能を備えてなる情報流通安全管理シ

テムの構成採用にある。

【0037】本発明システムの第7の特徴は、前記本発明システムの第2、第3、第4、第5又は第6の特徴における暗号鍵記憶部が、暗号化コンテンツ暗号鍵を記憶する機能を備えてなる情報流通安全管理システムの構成採用にある。

【0038】本発明システムの第8の特徴は、前記本発明システムの第1、第2、第3、第4、第5、第6又は第7の特徴における情報通信網が、インターネット、イントラネット（販売部を有する）、LAN、VAN、ISDN、VPN等を含んでなる情報流通安全管理システムの構成採用にある。

【0039】本発明システムの第9の特徴は、前記本発明システムの第1、第2、第3、第4、第5、第6、第7又は第8の特徴におけるセンタが、ストアやショップ、ショッピングセンタ、コミュニケーションセンタ、ショッピングモール、図書館、資料館、雑誌社、出版社、放送局、レコード会社、ゲームソフト会社、映画会社、新聞社等のヴァーチャル及びリアルを含んでなる情報流通安全管理システムの構成採用にある。

【0040】

【発明の実施の形態】本発明の実施の形態をその方法例及びシステム例につき図面を参照して説明する。本実施形態例では、文書情報や画像情報や音声情報やこれ等の組合せ情報の販売コンテンツをホームページ等を開設するストアやショップ、ショッピングセンタ、コミュニケーションセンタ、ショッピングモール、図書館、資料館、雑誌社出版社、放送局、ゲームソフト会社、映画会社、新聞社等のヴァーチャル及びリアルを含むセンタから、インターネット、イントラネット（販売部を有する）、LAN、VAN、ISDN、VPN等を含む情報通信網のネットワークシステムを通して、利用者端末に対し店頭公開するとともに、電子決算として電子クーポンや電子チケットや電子小切手やビットキャッシュやクレジットカードやサイバーコイン等の電子マネー残高を保管する電子財布を使用して電子商取引を行う場合を想定しているも、これに限定されるものではない。本発明の目的を達成し、後述する効果を有する範囲内においても適用可能である。

【0041】（システム例）本実施形態のシステム例を図1乃至図2について説明する。図1は本システム例を示す情報流通安全管理システムのブロック概念構成図、図2は同・外部装置内部の詳細ブロック構成図である。

【0042】本システムBは、センタ1と制御プログラム4'を保有する利用者端末5'と、復号プログラム2'及び電子財布3'を保有する外部装置6とからなり、センタ1と利用者端末5'間は情報通信網Nで接続される。なお、図4の従来システム例Aと同一構成ブロックは同一符号を付して説明の重複を避けた。

【0043】前記センタ1は、販売コンテンツMを品揃

え登録し、広告宣伝用コンテンツM'を店頭公開するとともに、購入要求に対し暗号化コンテンツ暗号鍵Kup [Ke]と暗号化販売コンテンツKe [M]をともども送信して見返りに受信した暗号化代金を復号化決算処理する機能を有する。

【0044】前記利用者端末5'は、制御プログラム4'に則って広告宣伝用コンテンツM'をアクセス閲覧してセンタ1へ購入要求を応信し、返信して来た暗号化販売コンテンツKe [M]と暗号化コンテンツ暗号鍵Kup [Ke]とを転信し、対価引出し支払を暗号化送信する機能を有する。

【0045】前記外部装置6は、制御プログラム4'に連携作動する復号プログラム2'と電子財布3'により、利用者端末5'から転送されて来た暗号化販売コンテンツKe [M]を先に又は同時に転送され事前に復号化した暗号鍵Keで復号化記憶するとともに記憶保持される電子マネーの代金差し引き残高を更新暗号化記憶する機能を有する。

【0046】それ故、当該外部装置6は、図2に示すよう、暗号化販売コンテンツKe [M]と暗号化コンテンツ暗号鍵Kup [Ke]を受信する端末入出力制御部7と、一連の復号、暗号及び記憶機能並びに代金差し引き残高保管記憶機能を統御する制御部8と、暗号化コンテンツ暗号鍵Kup [Ke]を復号する暗号鍵復号部9と、暗号化販売コンテンツKe [M]をコンテンツ暗号鍵Keで復号するコンテンツ復号部10と、マスター鍵Kmを記憶保持するマスター鍵記憶部11と、マネー、コンテンツM、コンテンツ暗号鍵Ke及び秘密鍵Kusの全情報をマスター鍵Kmで暗号化又は復号化する暗号／復号部12と、当該暗号化されたマネー情報を記憶するマネー情報記憶部13と、当該暗号化されたコンテンツ情報Km [M]を記憶するコンテンツ情報記憶部14と、当該暗号化されたコンテンツ暗号鍵Km [Ke]を記憶する暗号鍵記憶部15と、当該暗号化された秘密鍵Km [Kus]を記憶する秘密鍵記憶部16とで内部構成され、制御部8と暗号鍵復号部9とコンテンツ復号部10とマスター鍵記憶部11と暗号／復号部12は機密保護装置17に不可侵安全に内蔵される。

【0047】(方法例)当該本システム例に適用する本実施形態の方法例を図面について説明する。図3は本方法例の実行処理する手順動作シーケンスチャートである。

【0048】(1)初期条件

センタ1は、公開鍵暗号方式の秘密鍵Kcsを持ち、公開鍵Kcpを公開している一方、利用者端末5'は公開暗号方式の秘密鍵Kusを外装置6に持ち、公開鍵Kupを公開する。又、外部装置6の製造時には、機密保護装置17内のマスター鍵記憶部11に装置固有のマスター鍵Kmを書き込む。

【0049】他方、利用者端末5'の秘密鍵Kusは、

外部装置6の暗号／復号部12において、マスター鍵記憶部11に記憶してあるマスター鍵Kmで暗号化し、当該暗号化された秘密鍵Km [Kus]を秘密鍵暗号部16に書き込み、その上で、センタ1は利用者登録し、ある一定額の金券等を利用者端末5'に送信し、利用者はマネー情報記憶部13に暗号／復号部12でマスター鍵Kmにより暗号化してマネー情報記憶部13に格納する。

【0050】(2)センタ1の一次処理手順

まず、販売用のコンテンツMを登録して置く(ST1)。次いで、コンテンツMから利用者に無料で提供でき購買意欲を誘うような広告宣伝用コンテンツM'を生成する(ST2)。なお、情報提供者が広告宣伝用コンテンツM'を生成した後に、センタ1にコンテンツMを登録しても良い。広告宣伝用コンテンツM'は再編した、例えば、画像ならばサイズを小さくしたもの、ゲームならば体験版、音楽ならプログラム、映像ならば予告編版等のデータ転送の時間が余り掛からない程度のネットワークに負荷が小さいコンテンツM'とする。当該再編された広告宣伝用コンテンツM'を店頭公開する(ST3)。

【0051】(3)利用者の一次処理手順

まず、流通広告宣伝用コンテンツM'を利用者端末5'でホームページ等を検索して閲覧する(ST4)。次いで、購入する場合は購入要求をセンタ1に送信する(ST5)。

【0052】(4)センタ1の二次処理手順

利用者からの購入要求を受信すると、まず、コンテンツ暗号鍵Keを乱数表を用いてランダム生成する(ST6)。次いで、コンテンツMをコンテンツ暗号鍵Keで暗号化Ke [M]をする(ST7)。引続き、コンテンツ暗号鍵Keを利用者の公開鍵Kupで暗号化したコンテンツ暗号鍵Kup [Ke]と暗号化販売コンテンツKe [M]を利用者に送信する(ST8)。

【0053】(5)利用者の二次処理手順

(手順例1)利用者端末5'が暗号化コンテンツ暗号鍵Kup [Ke]と暗号化販売コンテンツKe [M]を受信すると、制御プログラム4'はまず、暗号化コンテンツ暗号鍵Kup [Ke]を外装置6に転送し、次いで端末入出力制御部7は、コンテンツ暗号鍵Kup [Ke]を転入し制御部8に引き渡す。

【0054】引続いて、制御部8は以降本処理手順の最終まで連続して駆動し続ける復号プログラム2'に則り、秘密鍵記憶部16に格納されている暗号化秘密鍵Km [Kus]を暗号／復号部12で復号し、暗号鍵復号部9において秘密鍵Kusで暗号化コンテンツ暗号鍵Kup [Ke]を復号する。制御部8は、暗号／復号部12においてマスター鍵Kmで暗号鍵Keを暗号化Km [Ke]し、暗号鍵記憶部15に格納する。

【0055】他方、制御プログラム4'は暗号化販売コ

コンテンツKe [M] を外部装置6に転送し、さらに、端末入出力制御部7は、暗号化販売コンテンツKe [M] を転入し、制御部8に引き渡す。その上で、制御部8は、さらに駆動し続ける復号プログラム2' に則り、暗号鍵記憶部15にある暗号化コンテンツ暗号鍵Km [Ke] を暗号/復号部12においてマスター鍵Kmで復号した後、制御部8は、コンテンツ復号部10において、取得した暗号鍵Keで暗号化販売コンテンツKe [M] を復号し(ST10)、取得したコンテンツMを暗号/復号部12にてマスター鍵Kmで暗号化しコンテンツ情報記憶部14に記憶させると同時にコンテンツMを端末入出力制御部7から利用者端末5' に出力する。

【0056】(手順例2) 利用者端末5' が暗号化コンテンツ暗号鍵Kup [ke] と暗号化販売コンテンツKe [M] を受信する(ST9)と、制御プログラム4' は、制御端末入出力制御部7を介して制御部8に暗号化コンテンツ暗号鍵Kup [Ke] と暗号化販売コンテンツKe [M] を同時に転送し、そのまま暗号/復号部12においてマスター鍵Kmでさらに暗号化し、ダブル暗号化コンテンツ暗号鍵Km {Kup [Ke]} とダブル暗号化販売コンテンツKm {Ke [M]} とをそれぞれコンテンツ情報記憶部14と暗号鍵記憶部15に格納する。

【0057】利用者は、コンテンツMを利用したい時に制御部8を動作して復号プログラム2' を駆動し、コンテンツ情報記憶部15から読み出したダブル暗号化販売コンテンツKm {Ke [M]} を暗号/復号部12においてマスター鍵Kmで復号化した後、一旦暗号化販売コンテンツKe [M] を端末入出力制御部7に出力して一度利用者端末5' の制御プログラム4' に戻す。その後

の手順は手順例1の【0055】以降の処理を行う。

【0058】(6) 電子決済処理
利用者の二次処理手順が終了すると利用者端末5' の制御プログラム4' は外部装置6の制御部8に電子財布3' のマネー情報記憶部13の電子マネー金券等残高を通知するよう命令して、読み出した暗号化金券等残高を暗号/復号部12においてマスター鍵Kmで復号した後、端末入出力制御部7を通して利用者端末5' に金券等残高情報が送られる。

【0059】次いで、制御プログラム4' は、通常の電子クーポン処理や課金モジュールの処理によりセンタ1に公開鍵Kcpで暗号化した代金を送信し(ST11)、コンテンツMの価格を差し引いた金券等残高情報を再度、外部装置6の端末入出力制御部7、制御部8、暗号/復号部12を経由してマネー情報記憶部13に更新格納する。他方、暗号化代金を送信されたセンタ1は、秘密鍵Kcsで復号し、コンテンツMの電子商取引に係わる決済処理(ST12)を実行して電子商取引を完了する。

【0060】

【発明の効果】かくして、本発明は、利用者端末側で制御プログラムを連携動作しかつ機密安全性を確保された外部装置の外部処理に復号解読と電子財布の管理を委ねるとともに、センタと、利用者端末間の情報流通を基本的には公開暗号鍵方式の採用の上で、情報配送時にセッション鍵で暗号化し、さらに外部装置の機密内領域の外部処理にマスター鍵を用いて本発明の電子商取引に三重安全管理体制を敷いて、情報流通における情報の安全保護を計る。

【0061】しかも、電子商取引を行うため、コンテンツの販売に先立って現実社会の商取引における広告宣伝同様、引き合い閲覧に負担にならず、知恵の出し所となる広告宣伝用のコンテンツを店頭公開流通して利用者の注意を喚起して購買意欲をそそり、より多くの顧客吸引力を発揮した上で、多くの購入要求を事前に得てから現物コンテンツを配信引き渡す電子商取引の合理化、効率化、安全化及び経済化を達成する等優れた効果を奏する。

【図面の簡単な説明】

【図1】本発明の実施の形態を示すシステム例の概念ブロック構成図である。

【図2】同上における外部装置内部の詳細ブロック構成図である。

【図3】本発明の実施の形態を示す方法例を実行処理する手順動作のシーケンスチャートである。

【図4】従来システム例の概念ブロック構成図である。

【図5】従来方法例を実行処理する手順動作のシーケンスチャートである。

【符号の説明】

A…従来システム例

B…本実施形態システム例

1…センタ

2, 2'…復号プログラム

3, 3'…電子財布

4, 4'…制御プログラム

5, 5'…利用者端末

6…外部装置

7…端末入出力制御部

8…制御部

9…暗号鍵復号部

10…コンテンツ復号部

11…マスター鍵記憶部

12…暗号/復号部

13…マネー情報記憶部

14…コンテンツ情報記憶部

15…暗号鍵記憶部

16…秘密鍵記憶部

Kcs, Kus…秘密鍵

Kcp, Kup…公開鍵

Ke…コンテンツ暗号鍵

15

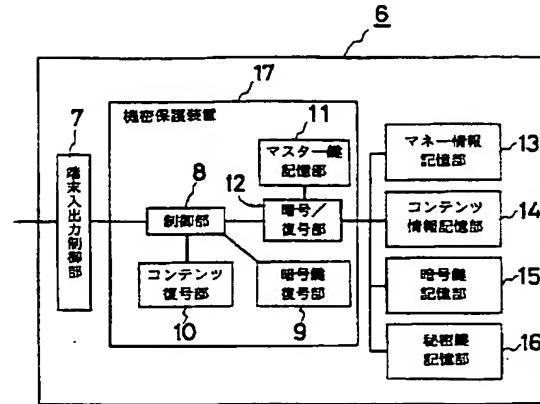
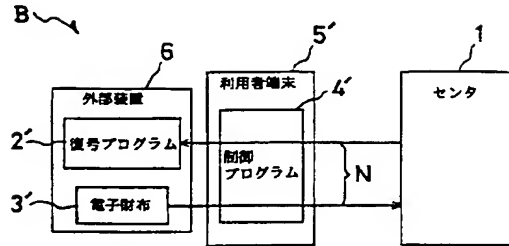
16

$K_e [M]$ …暗号化販売コンテンツ
 K_m …マスター鍵

M …コンテンツ
 M' …広告宣伝用コンテンツ

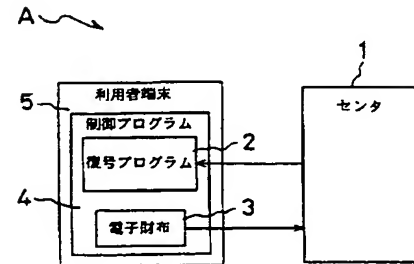
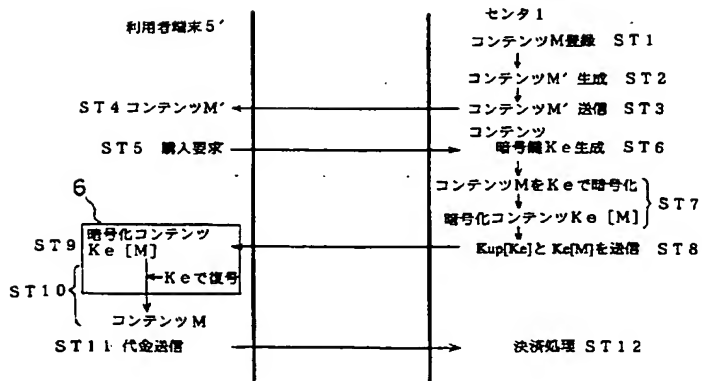
【図1】

【図2】

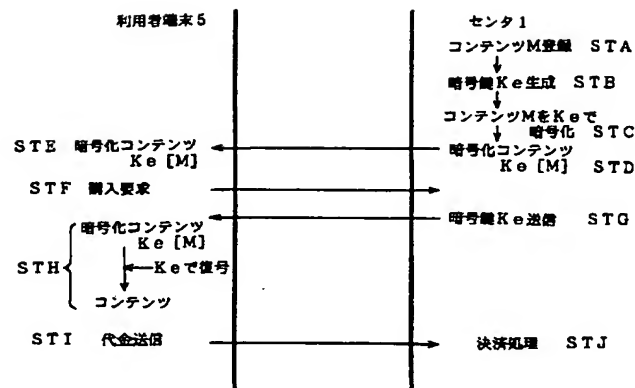


【図3】

【図4】



【図5】



フロントページの続き

(72)発明者 山中 喜義
東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内

(72)発明者 松本 博幸
東京都渋谷区桜丘町20番1号 エヌティテ
ィエレクトロニクス株式会社内